corresponding to US 2002/0046189 A1

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－123779
（P2002－123779A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	４１４ ＺＥＣ	Ｇ０６Ｆ　17/60	４１４ ＺＥＣ	５Ｂ０４９

審査請求　未請求　請求項の数18　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－316856(P2000－316856)

(22)出願日　平成12年10月12日(2000.10.12)

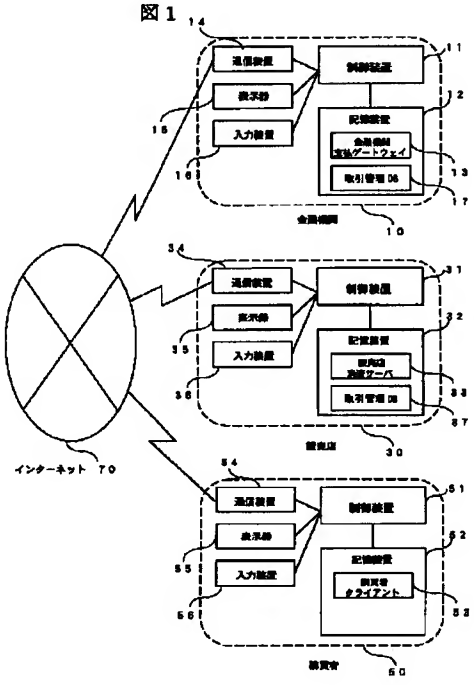
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　森田　光
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(72)発明者　千葉　寛之
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　決済処理方法及びシステム並びにプログラムを格納した記録媒体

(57)【要約】
【課題】決済の確実性、安全性、迅速性のバランスを考慮した決済方法及びシステム並びにプログラムを記録した記録媒体を提供する。
【解決手段】クレジット会社、銀行等の金融機関において、決済当事者たる販売店からの決済内容情報（取引内容情報）と、決済当事者たるユーザからの決済内容（取引内容）に応じて変化する認証情報とを用いて、決済要求が有効か否かを判断する。そして、前記販売店から送信される決済内容情報と、前記認証情報から抽出される決済内容情報とが異なっている場合は、決済要求を不可とする。

図１



1

【特許請求の範囲】

【請求項１】決済処理システムを利用した決済処理方法であって、前記決済処理システムを介して決済を行うユーザのユーザＩＤと前記ユーザの本人性確認情報とを対応付けてデータベースで管理し、前記ユーザＩＤと、前記決済の決済内容情報と、当該決済内容情報と前記本人性確認情報とを用いてユーザにより作成される認証情報とを受け、前記ユーザＩＤに対応する本人性確認情報を前記データベースから抽出し、前記本人性確認情報と前記決済内容情報と前記認証情報とを用いて前記決済の要求が有効か否かを判定することを特徴とする決済処理方法。

【請求項２】請求項１記載の決済処理方法であって、前記認証情報は、ハッシュ関数により作成されたハッシュ値であることを特徴とする決済処理方法。

【請求項３】決済処理システムを利用した決済処理方法であって、前記決済処理システムを介して決済を行うユーザのユーザＩＤと前記ユーザの本人性確認情報とを対応付けてデータベースで管理し、前記ユーザＩＤと、前記決済の決済内容情報と前記本人性確認情報とを用いてユーザにより作成される認証情報とを受け、前記ユーザＩＤに対応する本人性確認情報を前記データベースから抽出し、前記本人性確認情報と前記認証情報とを用いて決済内容を特定することを特徴とする決済処理方法。

【請求項４】債権者側システムと通信手段で接続され、当該通信手段を介して送信される決済要求に応答する金融機関側システムにおける決済処理方法であって、前記債権者側システムにより作成される決済内容情報と、前記債権者との決済対象者である債務者により作成され、決済内容に応じて変化する認証情報とを受け、前記決済内容情報と前記認証情報とに基づき決済要求が有効か否かを判断することを特徴とする決済処理方法。

【請求項５】請求項４記載の決済処理方法であって、前記認証情報は前記決済内容の一部を欠落させた情報であり、前記金融機関システムは、前記債権者側システムにより作成される決済内容情報から情報の一部を欠落させ、前記認証情報と比較することによって決済要求が有効か否かを判断することを特徴とする決済処理方法。

【請求項６】請求項５記載の決済処理方法であって、前記認証情報は、ハッシュ関数により作成されたハッシュ値であることを特徴とする決済処理方法。

【請求項７】販売店側システムと通信手段で接続され、当該通信手段を介して送信される決済要求に応答する金融機関側システムにおける決済処理方法であって、前記金融機関を介して決済を行うユーザのユーザＩＤと前記ユーザの本人性確認情報とを対応付けてデータベースで管理し、前記販売店側システムから販売店との決済対象者を特定する前記ユーザＩＤ、決済内容情報、当該決済内容情報と前記本人性確認情報とを用いてユーザにより作成される加工認証情報を受け、前記ユーザＩＤに対応する本人性確認情報を前記データベースから抽出し、前記本人性確認情報と前記決済内容情報と前記加工認証情報とを用いて前記決済要求が有効か否かを判定することを特徴とする決済処理方法。

2

【請求項８】請求項７記載の決済処理方法であって、前記販売店側システムから送信される決済内容情報と、前記加工認証情報から抽出される決済内容情報とが異なっている場合は、決済要求を不可とすることを特徴とする決済処理方法。

【請求項９】請求項７記載の決済処理方法であって、前記決済内容情報は決済金額情報であり、前記加工認証情報は前記決済金額情報と前記本人性確認情報とを用いて所定の条件により計算を行ったものであることを特徴とする決済処理方法。

【請求項１０】請求項９記載の決済処理方法であって、前記加工認証情報は、前記販売店側システムと通信手段で接続されるユーザ側システムで作成されることを特徴とする決済処理方法。

【請求項１１】請求項１０記載の決済処理方法であって、前記加工認証情報は一方向性関数により作成されたものであり、前記金融機関側システムと前記ユーザ側システムとは予め前記所定の条件を共有していることを特徴とする決済処理方法。

【請求項１２】ユーザ側システム及び販売店側システムと通信手段で接続され、当該通信手段を介して送信される決済要求に応答する金融機関側システムにおける決済処理方法であって、前記金融機関を介して決済を行うユーザＩＤと当該ユーザの本人性確認情報とを対応付けてデータベースで管理し、前記販売店システムから送信される前記ユーザＩＤ及び決済内容情報と、前記ユーザ側システムで前記本人性確認情報と前記決済内容情報とを用いて作成される加工認証情報とを受け、前記本人性確認情報と前記決済内容情報と前記加工認証情報とを用いて決済要求の可否を判定することを特徴とする決済処理方法。

【請求項１３】ユーザ側システム及び販売店側システムと通信手段で接続され、当該通信手段を介して送信される決済要求に応答する金融機関側システムにおける決済処理方法であって、前記金融機関を介して決済を行うユーザＩＤと当該ユーザの本人性確認情報とを対応付けてデータベースで管理し、前記販売店システムから前記ユーザＩＤと決済内容情報とを受けて、前記販売店システムへ第1の情報を送信すると共に当該第１の情報と前記ユーザＩＤとを対応付けて管理し、前記ユーザＩＤ、前記第１の情報と前記本人性確認情報と前記決済内容情報とを用いてユーザにより作成される第２の情報を受け、前記本人性確認情報と前記決済内容情報と前記第１の情報と前記第２の情報とを用いて決済要求の可否を判定することを特徴とする決済処理方法。

【請求項１４】請求項１３記載の決済処理方法であっ

て、前記第１の認証情報は可変情報であることを特徴とする決済処理方法。

【請求項１５】販売店側システムと通信回線で接続され、当該通信回線を通じて送信される決済要求に応答する決済処理システムであって、当該決済処理システムを介して決済を行うユーザのユーザＩＤと前記ユーザの本人性確認情報とを記録する記憶装置と、前記販売店側システムから販売店との決済対象者を特定する前記ユーザＩＤ、決済内容情報、当該決済内容情報と前記本人性確認情報とを用いてユーザにより作成される加工認証情報を受ける通信装置と、前記ユーザＩＤに対応する本人性確認情報を前記記憶装置から抽出し、前記本人性確認情報と前記決済内容情報と前記加工認証情報とを用いて前記決済要求が有効か否かを判定する制御装置とを備えたことを特徴とする決済処理システム。

【請求項１６】通信手段で接続された金融機関側システムに対し、決済要求を送信するシステムであって、決済内容に応じて変化する認証情報を作成する手段と、当該認証情報を送信する手段とを備えたことを特徴とするシステム。

【請求項１７】請求項１６記載のシステムであって、前記認証情報は、前記金融機関を介して決済を行うユーザの本人性確認情報と前記決済内容とを用いて作成される情報の一部を欠落させた情報であることを特徴とするシステム。

【請求項１８】販売店側システムと通信手段で接続され、当該通信手段を介して送信される決済要求に応答する金融機関側システムで用いられる決済処理プログラムを格納した記録媒体であって、前記金融機関を介して決済を行うユーザのユーザＩＤと前記ユーザの本人性確認情報とを対応付けてデータベースで管理する機能と、前記販売店側システムから販売店との決済対象者を特定する前記ユーザＩＤ、決済内容情報、当該決済内容情報と前記本人性確認情報とを用いてユーザにより作成される加工認証情報を受け、前記本人性確認情報と前記決済内容情報と前記加工認証情報とを用いて前記決済要求が有効か否かを判定する機能とを備えたことを特徴とする決済処理プログラムを格納した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、 商取引に用いられる決済処理方法及びシステム並びにプログラムを格納した記録媒体に係り、特に安全な商取引を行うために、決済内容に応じて変化する情報に基づいて、決済当事者からの決済要求を処理する決済処理方法及びシステム並びにプログラムを格納した記録媒体に関する。

【０００２】

【従来の技術】近年、購買者がネットワークを利用して、販売店へ商品やサービスの購入依頼を行うオンライン取引が様々な形で提供されている。このオンライン取引における決済方法には、例えば特開２０００－１４８８５４号公報に開示されているように購買者がオンライン取引に係る代金を金融機関へ直接振込依頼する方法と、販売店から金融機関に対して決済要求を行う、いわゆる「オンライン決済」と呼ばれる方法とがある。現在のオンライン決済では、クレジットカードが多く利用されている。オンライン決済でクレジットカードを利用する場合には、購買者が販売店へ購買者のクレジットカード番号を知らせ、当該カードによる決済処理を依頼し、販売店が決済機関であるクレジットカード会社に対して、商品代金に対する支払承認処理（いわゆるオーソリゼーション、キャプチャなどの与信処理)を行うことによって、カード会社の承認に基づく商品売買を行っている。

【０００３】

【発明が解決しようとする課題】しかしながら上述した従来技術では、オンライン取引に係る決済の確実性、安全性、迅速性への配慮が十分とは言えなかった。購買者が金融機関へ直接振込依頼する方法では、販売店は、振込状況を把握するために振込依頼内容を問い合わせ、適切な金額が振り込まれているか否かを確認するといった作業負荷が発生する。また、振込依頼内容が異なっていた場合には、購買者への連絡等の煩雑な手続きが生じる。購買者にとっても、振込みが確実に行われたか、その結果決済が確実に行われたかといった振込み後の確認作業や、振込依頼内容が異なっていた場合の処理は煩雑である。

【０００４】一方、オンライン決済では、決済可能か否かの判断は金融機関を介して比較的スムーズに行われる。しかし、このような決済サービスをインターネットなどのオープンネットワークを用いて実現する上では、クレジットカード番号等の個人情報の漏洩を防ぐといった安全性の確保が不可欠であるが、例えSSL(Secure Socket Layer)/ TLS(Transport Layer Security) のような暗号路生成技術に頼ったとしても、クレジットカードを用いた決済においては、購買者が販売店に対して、クレジットカード番号を通知することになる。クレジットカードを用いた決済の場合は、購買者は、実際に決済代金を支払う前に、クレジットカード会社からの請求内容の妥当性を、カード利用明細書を用いて判断する事ができるので、万一請求内容が不適当な場合には、面倒な手続きであるが支払を拒否することができる。しかし、デビットカードやキャッシュカードなどを利用した決済に代表される即時決済においては、決済の実施が即時であるため、クレジットカード決済のような請求内容の確認という事後のプロセスすらない。そのため、金融機関は決済実施前に厳密に本人確認を行う必要があり、例えば銀行口座からの即時決済のように、本人確認方法として口座番号と購買者のみが知り得る情報（暗証情報）を用いることとなるが、購買者－販売店－決済機関という

三者に跨った即時決済を、クレジット決済と同様な仕組みで行おうとすると、 購買者は、口座番号と暗証情報を販売店に送信することになり、暗証情報を第三者に教えることになる。これらは、オンライン取引に限らず、現実の取引におけるクレジットカード決済等でも生じる問題でもある。

【０００５】そこで、特開平１０－３２６３１０号公報に開示されるような１回限りの決済に有効な暗証情報（都度変更情報）を用いる方法が考えられる。しかし、上記公報において、金融機関は、販売店から与えられる取引に係る請求情報にのみ基づいて決済を行っているため、販売店の請求内容が不適当であった場合、購買者は不利益を被ることとなる。また、暗証情報は、購買者主導で随時変更されるため、なりすましを防止することが出来ない。

【０００６】本発明の目的は、決済の確実性、安全性、迅速性のバランスを考慮した決済方法及びシステム並びにプログラムを記録した記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明ではクレジット会社、銀行等の金融機関（決済処理機関）において、決済当事者たるユーザ（債務者、購買者等）からの決済内容（取引内容）に応じて変化する認証情報を用いて、決済要求が有効か否かを判断したり、決済内容を特定したりすることを特徴とする。ここで、決済には、振込、振替、クレジット決済、デビット決済、手形決済等を含む。これにより、認証情報に決済内容が反映されているので、本人が意図した決済を安全確実に行うことができる。

【０００８】また、決済当事者たる債権者（販売店等）からの決済内容情報（取引内容情報）と、決済当事者たるユーザ（債務者、購買者等）からの決済内容（取引内容）に応じて変化する認証情報とを用いて、決済要求が有効か否かを判断することを特徴とする。これにより、販売店が要求している決済内容とユーザが指示している決済内容とが一致していることを決済機関たる金融機関が容易に確認することができる。また、これらの手法を用いることにより、金融機関によるユーザの本人性確認を、金融機関以外の第三者に送信しても構わない情報、つまり固定的でなく都度変化する可能性があるため秘匿性を強く要求されない認証情報で実施できる。また、ユーザの認証情報が第三者を経由して金融機関へ伝えられた場合でも、 ユーザの本人性確認ならびに決済内容確認を確実に実施することができるため、 安全確実な決済を実現することができる。さらに、個人情報の漏洩防止にもつながる。ここで、決済内容（取引内容）情報には、取引商品情報、取引サービス情報、販売店情報、取引日時情報、決済金額（取引金額）に関連する情報等がある。

【０００９】より具体的には、債権者（販売店）側システムと通信手段で接続され、通信手段を介して送信される決済要求に応答する決済処理システムであって、前記決済処理システムを介して決済を行うユーザ（債務者）のユーザＩＤ（決済用識別子、取引用識別子、クレジットカード番号、金融機関の口座番号等も含む）と前記ユーザの本人性確認情報（例えば、クレジットカード番号自体、クレジットカード番号に対応付けられた暗証番号、暗証フレーズ等であり、取引内容に対して固定的な認証情報）とを対応付けてデータベースで管理し、販売店側システムから販売店との決済対象者を特定する前記ユーザＩＤ、決済内容情報、当該決済内容情報と前記本人性確認情報とを用いてユーザにより作成される加工認証情報（取引内容に応じて可変的な認証情報であり、例えば一方向ハッシュ関数等を用いる）を受け、前記ユーザＩＤに対応する本人性確認情報を前記データベースから抽出し、前記本人性確認情報と前記決済内容情報と前記加工認証情報とを用いて前記決済要求が有効か否かを判定することを特徴とする。そして、前記販売店側システムから送信される決済内容情報と、前記加工認証情報から抽出される決済内容情報とが異なっている場合は、決済要求を不可とすることを特徴とする。

【００１０】尚、上記目的を達成するためには、上述した機能を実現するプログラム若しくはプログラムを格納した記録媒体であっても良い。

【００１１】

【発明の実施の形態】以下本発明の実施の形態を、 図面を参照しながら詳細に説明する。以下の例は、ネットワークを通じて商品売買を行い、それを金融機関で決済するシステムに、本発明を適用した場合のものである。

【００１２】図１は、本発明の一実施形態による電子商取引システムの構成図である。

【００１３】この電子商取引システムは、購買者（ユーザ）システム５０と、販売店システム３０と、金融機関システム１０を含んで構成される。尚、本実施例では、商品売買を例にしているので、購買者は送金者（債務者）に、販売店は受領者（債権者）に、金融機関は決済機関にそれぞれ該当する。

【００１４】これらは、インターネットのようなネットワーク、公衆網、専用網等の通信手段７０を介して接続される。

【００１５】購買者システム５０は、インターネット等のネットワークに接続可能なパソコン、携帯端末等である。購買者システム５０には、購買者（ユーザ）が情報を入力するキーボードやマウスといった入力装置５６と、情報を表示する表示器５５と、インターネット等のネットワークを介して通信を行う通信装置５４とを備えているほうが望ましい。記憶装置５２は、キャッシュ、メモリ等の主記憶装置やハードディスク等の外部記憶装置を含む。また、購買者クライアント５３は、HTTP(Hyp

ertext Transfer Protocol）に基づいた通信を行う Web ブラウザ機能（指定ＵＲＬへのアクセス機能、指定リソースをローカル記憶装置へ保存する機能等）を有しており、 また必要な情報を基に、後述するワンタイムパスワード（認証情報）を生成することができる。この購買者クライアント５３の機能の一部は、ＪＡＶＡ（登録商標）等を用いて金融機関システム等から提供するようにしても良い。このようにすることによって、本システムを用いる際の利用者負担が軽減する。制御装置５１は、これら全ての制御及びプログラム処理に関連する。

【００１６】販売店システム３０には、購買者システム５０における各機能と同様の性質を有する入力装置３６、表示器３５、通信装置３４、記憶装置３２、制御装置３１の他、HTTP に基づいた通信を行う機能を有しており、購買者クライアント５３や金融機関支払ゲートウェイ１３などと通信を行う販売店決済サーバ３３を備える。販売店決済サーバ３３は、受信データをローカル記憶装置に格納したり、ローカル記憶装置内のデータを送信したりする機能も有している。また、後述するデータを有する取引管理データベース３７を管理している。

【００１７】金融機関システム１０には、購買者システム５０における各機能と同様の性質を有する入力装置１６、表示器１５、通信装置１４、記憶装置１２、制御装置１１の他、HTTP に基づいた通信を行う機能を有しており、販売店決済サーバ３３などと通信を行う金融機関支払ゲートウェイサーバ１３を備える。金融機関支払ゲートウェイサーバ１３は、受信データをローカル記憶装置に格納したり、ローカル記憶装置内のデータを送信したりする機能も有している他、後述するワンタイムパスワードを生成する機能、ネットワークを経由して入手したワンタイムパスワードとローカルで作成したワンタイムパスワードとの比較を行う機能も有している。また、後述するデータを有する取引管理データベース１７を管理している。この金融機関システム１０の機能の一部を、サービスプロバイダー等によりアウトソーシングするような構成としても良い。

【００１８】尚、上述した購買者システム５０、販売店システム３０、金融機関システム１０の各々の機能は、ソフトウェアとしても提供可能であり、例えば金融機関支払ゲートウェイ１３の一機能を実現するプログラムを格納する記憶媒体を設け、このプログラムを金融機関システム１０に接続される駆動装置（図示しない）を介して金融機関システム２０のメモリに読み込むか、インターネット７０を介して金融機関システム１０へ伝送して、実行すること等が可能である。

【００１９】本発明の概略を説明する。図 1に示す購買者システム５０を利用するユーザは、金融機関とオンラインショッピング決済の利用契約を結び、後述するワンタイムパスワードを用いて決済する旨の合意を予め得ておく。また、少なくとも金融機関を介して取引の決済を行う前に、ワンタイムパスワードの計算に用いる所定の条件（計算式等）を金融機関と共有しておく必要がある。次に、ユーザは、販売店システム３０を利用する販売店との間で、 商品の購入といった決済が必要となる交渉を行い、この決済要求指示を金融機関１０に対して行う。この際、ユーザは、金融機関がユーザを正しく確認をすること、ならびに、決済金額等といったユーザが販売店と交渉した内容（決済内容情報)を金融機関が正しく確認することができるように、 決済内容情報と関連性を持った認証情報を作成し、決済要求指示を実行する。金融機関は、この認証情報に基づいて決済要求指示の有効性を判断するため、取引の安全性、確実性が向上することになる。本明細書では、この決済内容情報と関連性を持った認証情報をワンタイムパスワード（加工認証情報）と記述する。このワンタイムパスワードは、決済内容情報と関連性を持った認証情報であるため、決済内容に応じて可変な認証情報である。そのため、例え第三者へ情報が漏洩したとしても安全性は高い。しかし、安全性をより向上させるべく、認証情報の秘匿性を追求する場合は、ワンタイムパスワードをＳＳＬ／ＴＬＳといった暗号路生成技術を用いて暗号化することやSECE（SecureElectronic Commerce Environment）と呼ばれる決済方式の中に取り入れることも考えられる。その中でも、最も効果が期待されるものは、ワンタイムパスワードの生成に一方向性関数（ハッシュ関数）を用いる方法である。図１２に示すとおり、一方向性関数の計算では、入力値（例えば、クレジットカード番号に対応づけられた暗証フレーズがｐａｓ１、取引の決済金額が１５００とする）に対して出力値（ｉ＞）を求める際、入力値から得られる情報の一部を欠落させる（１２０４）。従って、出力値から入力値を導き出すことが不可能となり、出力値をワンタイムパスワードとして用いると、第三者は入力値（本例では、暗証フレーズ及び取引の決済金額）に対する不正を働くことが出来ない。さらに、図１２の１２０２、１２０４から明らかなように、一方向性関数を用いると入力値に対して出力値のデータ量を圧縮させることができるため、出力値をワンタイムパスワードとして用いることにより伝送データ量を削減し、通信のトラフィックの増大を抑制することができるといった効果も生じる。これは、取引の確実性・安全性を向上させるために伝送データ量が増大し、各システムにおいて取り扱うデータ量が増大するのを抑制する効果となる。その結果、決済応答も迅速に行えることとなり、取引における決済処理には大変重要なことである。但し、ワンタイムパスワードを用いることにより取引の確実性・安全性を向上させるといった効果は、例えばクレジットカード番号等に対応づけられた暗証フレーズ（本人性確認情報であれば他の情報であっても良い）と取引内容を特定する情報（決済金額に関連する情報が望ましいが、単なる取引商品情報、取引サービス情報、販

売店情報、取引日時情報等であっても、取引内容をある程度特定できるので、それなりの効果は期待できる）との単純な演算（単なる加算、減算等）や、暗証フレーズへのデータの単なる付加（例えば、決済金額から導き出されるチェックディジットの付加等）により作成されるワンタイムパスワードであっても、ユーザと金融機関以外の第３者の知り得ない作成方法である限り、生じている点を追記しておく。

【００２０】次に本発明をより具体的に説明する。図２は、金融機関システム１０の取引管理ＤＢ１７のデータ構成を示す図である。なお、これらのデータベース構成は、実施の一例であり、管理方法にはバリエーションがある。金融機関では、購買者である顧客とのオンライン決済取引契約に基づき、各顧客毎に、ユーザ識別子（ユーザＩＤ）２０１、決済に用いる口座の口座番号（クレジット番号）２０２、口座番号に対応し、本人性確認情報として用いられる暗証情報である暗証フレーズ２０３を含む顧客管理データ２００を予め管理している。本例でのユーザ識別子２０１は、主にインターネット取引で用いるための識別子を想定しているが、口座番号２０２を識別子として用いても良い。また、金融機関は、販売店との加盟店契約に基づき、各販売店毎に、販売店を特定する販売店識別子２１１、決済に用いる口座番号２１２を含む販売店管理データ２１０を予め管理している。さらに、各取引毎に、決済トランザクション管理に用いる取引識別子２２１、決済の実施に必要な、資金移動元である購買者、資金移動先である販売店、決済金額を特定するための、ユーザ識別子２２２、販売店識別子２２３、決済金額２２４を含む取引管理データ２２０を管理する。尚、本実施例では、後述する暗証加工情報（チャレンジ）２２５を各取引毎に対応づけて管理している。暗証加工情報を各顧客毎に対応づけて管理しても良いが、同一顧客による複数取引といった多重処理に対処するには、各取引毎に対応づけて管理するほうが望ましい。

【００２１】図３は、販売店システム３０の取引管理ＤＢ３７のデータ構成の一例を示す図である。販売店では、金融機関との加盟店契約に基づき、各金融機関毎に、金融機関から割り当てられた販売店識別子３１３、金融機関への接続先情報３１２を含む金融機関データ３１０を予め管理している。また、商品売買に伴う決済情報として、各取引毎に、決済トランザクション管理に用いる取引識別子３０１、決済金融機関３０２、ユーザ識別子３０３、購入金額３０４、取引（決済）の状況を管理する取引ステータス３０５を含む決済用取引管理データ３００を管理する。購買者と金融機関との間の決済に関連する情報の仲介（転送を含む）を販売店が行う方法を採用すると、この取引ステータスを随時更新し、取引状況をより詳細に把握できるため、販売店にとっては望ましいものとなる。

【００２２】尚、販売店は、取引識別子３２１、商品３２２、数量３２３、ユーザ送付先３２４を含む商品販売取引管理データ３２０も管理する。

【００２３】図４は、本発明を用いた電子商取引システムのショッピングフローを示したものである。購買者は、販売店と商品売買交渉を行い、なんらかの決済が必要となると決済方法（クレジットカード決済、デビットカード決済等）を選択する（４０１）。次に、購買者は、金融機関が購買者を特定するための識別子（ユーザＩＤ、クレジットカード番号等）を、決済金融機関を特定する情報と共に販売店へ通知する（４０２）。販売店は、金融機関が購買者を特定するための識別子、決済金額等の決済情報、ならびに、金融機関が販売店を特定するための販売店識別子を送信し、購買者が決済を行おうとしていることを金融機関へ通知する（４０３）。次に、販売店は、金融機関から、購買者がワンタイムパスワードを作成する際に用いる暗証加工情報（チャレンジ）を受信し（４０４）、購買者へ送信する（４０５）。ここで、暗証加工情報とは、通知の都度変化する値であり、ワンタイムパスワードを生成する際に用いるデータである。暗証加工情報の例としては、通知の度に増加（減少）する番号やバイナリデータを含むランダム値などが挙げられる。この暗証加工情報は、ワンタイムパスワードの安全性をより強固なものとすべく用いるものであるため、ワンタイムパスワードの使用条件（例えば、決済金額が大きい、頻繁に決済に用いられる等）に応じて暗証加工情報を用いるか否か選択できる。

【００２４】購買者は、ワンタイムパスワードを生成し、販売店へ送信する（４０６）。販売店は、購買者から受信したワンタイムパスワードを金融機関へ送信し、決済を依頼する（４０７）。金融機関は、ワンタイムパスワードを検証することで、購買者の本人確認ならびに、 購買者と販売店の間で決済情報が一致しているかを確認し、決済の可否を販売店へ返信する（４０８）。販売店は、決済の可否を確認することで取引の成否を決定し、その結果を購買者へ通知する（４０９）。このように購買者と金融機関との間の決済に関連する情報の仲介を販売店が行うことによって、販売店は取引（決済）状況を迅速に把握することができる。

【００２５】次に、購買者、販売店、金融機関における処理フローを、順に説明する。

【００２６】図５は、購買者のフローを示したものである。購買者は、販売店からの商品購入にあたり購入内容を確認し、販売店が提示した決済に利用できる金融機関リストから、本決済を行う金融機関を選択する。さらに、この選択された金融機関情報と、当該金融機関でオンライン決済を利用する際に用いる購買者特定情報（ユーザID、口座番号等のうち少なくとも１つ）を販売店へ送信し、販売店へ当該金融機関による決済意思を示すとともに、当該金融機関への暗証加工情報の販売店による

代理取得を依頼する（５０１：購入開始要求の送信）。次に、ステップ５０１の購入意思表示の応答として、購買者が指定した金融機関が生成した暗証加工情報を、販売店経由で受信する（５０２：購入開始応答の受信）。次に、オンライン決済に用いるユーザID、受信した暗証加工情報、販売店との間で合意した決済金額、購買者と金融機関のみが知っている暗証フレーズ（本人性確認情報）を用いて、ワンタイムパスワードを生成する（５０３）。ここでは、ワンタイムパスワードの作成に、一方向性ハッシュ関数を用いる。つまり、上記情報を入力として一方向性ハッシュ関数を適用して得られるハッシュ値を、ワンタイムパスワードとして用いる。次に、購買者は、金融機関へ対して決済金額にしたがった決済を指示する目的で、ユーザID、ステップ５０３で生成したワンタイムパスワードを、購入要求として販売店へ送信する（５０４：購入要求の送信)。ステップ５０４の購入要求の応答として、購買が成立したかどうかを示す購買結果を販売店から受信し、販売店との取引の成否ならびに金融機関での決済の結果を確認する（５０５：購入応答の受信)。

【００２７】図６は、販売店のフローを示したものである。販売店は、決済可能な金融機関リストを購買者に提示することで、購買者が決済に利用する金融機関を指定させ、購買者の決済意思ならびに利用金融機関を特定する。また、購買者が当該金融機関で決済を実施するのに必要な暗証加工情報を購買者に代って請求するために、当該金融機関が購買者を特定するためのユーザID を受信する（６０１：購入開始要求の受信）。次に、暗証加工情報を代理取得するために、購買者が選択した金融機関へ対して、ステップ６０１で受信したユーザID、購買者との間で合意された決済金額、ならびに、購買者からの決済金額を受け取るための販売店口座特定情報（販売店ID）を送信する（６０２： 暗証加工情報要求の送信）。ステップ６０２の応答として、金融機関から、当該顧客が金融機関に対して決済を指示する際に使用する暗証加工情報を受信する（ステップ６０３：暗証加工情報応答の受信）。ステップ６０１で受信した購入開始要求の応答として、暗証加工情報を購買者へ送信する（６０４：購入開始応答の送信）。購買者から、購入意思表示として、今回の取引のために生成されたワンタイムパスワードとユーザIDを、購入要求として受信する（６０５：購入要求の受信）。次に、販売店は、金融機関へ対して、購買者から受信したワンタイムパスワード、ユーザID を送信し、決済を依頼する（６０６：決済要求の送信）。ステップ６０６の決済要求の応答として、決済結果を受信する。この決済結果に基づき、取引の成否を判断し、必要に応じて商品発送などのサービス提供を行う(６０７：決済応答の受信)。ステップ６０７の取引の成否の判断結果を、取引結果として購買者へ送信する（６０８：購入応答の送信）。

【００２８】図7は、金融機関のフローを示したものである。販売店から、購買者のユーザID、決済金額、販売店口座特定情報(販売店ID)を受信する（７０１：暗証加工情報要求の受信）。ここで受信した決済金額は、購買者との間で合意したと販売店が主張する金額である。また、金融機関は、販売店 ID を利用し、決済を実施する際の資金移動先を特定する。次に、ユーザIDから購買者を特定し、当該購買者に対して適切な暗証加工情報を生成し、暗証加工応答として販売店へ送信する（７０２：暗証加工情報応答の送信）。販売店から、決済要求として、ユーザID、ワンタイムパスワードを受信する（７０３：決済要求の受信）。次に、ワンタイムパスワードを検証する（７０４、７０５：ワンタイムパスワードの検証）。この検証は、販売店から受信した購買者作成のワンタイムパスワードと、金融機関が、購買者のユーザID、販売店から受信した決済金額、現在有効な当該購買者の暗証加工情報、事前に登録されている購買者の暗証フレーズを用いて作成したワンタイムパスワードとが一致するかを比較することである。ここで、現在有効な暗証加工情報とは、ステップ ７０２で送信した暗証加工情報を指す。ここでは、購買者の場合と同様に、ワンタイムパスワードの検証に、一方向性ハッシュ関数を用いる。つまり、上記情報を入力として一方向性ハッシュ関数を適用し、ハッシュ値を得る。このようにして得られたハッシュ値と、受信したワンタイムパスワードとの比較を行い、両者が一致することを確認する検証処理を行う。ステップ７０５の比較の結果、両者が一致すれば、決済要求成功と判断する(７０６)。決済要求成功の場合は、通常行われているように決済可能な状態かを判断し（７０８）、可能であれば決済処理を行う（７１０）。決済処理を行うとは、ユーザIDにより特定される顧客口座から、販売店IDにより特定される販売店口座に、決済金額で指定される金額を移動させること（クレジットカード決済の場合は、支払承認）を指す。一方、ステップ７０５の比較の結果、両者が一致しなければ、決済要求失敗と判断し（７０７）、決済処理を行わない（７０８）。決済が失敗する要因としては、顧客が指定した購入金額と、販売店が指定した購入金額が異なっていることや、暗証フレーズが異なっている、つまり、暗証フレーズの入力ミスや、暗証フレーズを知らないものがワンタイムパスワードを生成したことや、 ワンタイムパスワードを生成した際の暗証加工情報が、現在は有効でない等が挙げられる。

【００２９】最後に、ステップ７０９、７１０の決済結果を、決済応答として販売店へ送信する（７１１：決済応答の送信）。

【００３０】図８は、 購買者システム５０の表示器５５上に表示された購入開始要求を送信する際のクライアント表示を示す図である。販売店によって提示された決済金融機関のリストのから、決済に用いる金融機関を入

力装置５６を介して選択する。また、当該金融機関でのユーザID（図８における「デビット契約番号」） を入力した後、「決定」ボタンを指示し、選択した銀行情報と入力したユーザID を、購入開始要求として販売店へ送信し、上記口座による決済の意思を示す。

【００３１】図９は、購買者システム５０の表示器５５上に表示された購入要求を送信する際のクライアント表示を示す図である。購入開始応答を受信すると、購買者クライアントは、購入金額（決済金額）、ユーザID、暗証フレーズの入力を促す。上記項目が入力された後「支払」 ボタンが指示されると、入力された情報ならびに暗証加工情報に基づきワンタイムパスワード生成処理が開始され、 生成したワンタイムパスワードとユーザIDを、購入要求として販売店へ送信し、指定した金融機関からの代金支払による商品購入を依頼する。

【００３２】図１０は、購買者５０の表示器５５上に表示された購入応答を受信した際のクライアント表示を示す図である。この図は、購入要求として送信した購入の結果を示しており、これによって購買者は、購入要求で指定した取引に関して、購買者が指定した金融機関から購入代金が支払われ、販売店との取引が成立したことを確認することができる。

【００３３】なお、上記実施形態では、購買者の本人性ならびに決済情報を代表する都度変化する代替情報であるワンタイムパスワードとして、計算により求められたハッシュを挙げたが、上記の目的に沿うのであれば、ハッシュの代わりに他の方式によって生成した代替情報であっても良い。

【００３４】また、上記実施形態では、金融機関が決済金額を特定するための情報として購入金額を、金融機関が購買者（顧客）を特定するための情報としてユーザIDを、それぞれワンタイムパスワードの生成のための一要素として用いたが、上記目的に沿うのであれば、 購入金額の代わりに購入商品情報など他の情報を、また、ユーザID の代わりにユーザID と結び付けられた顧客保有口座番号などの他の情報を用いてワンタイムパスワード生成を行うことができる。

【００３５】さらに、上記実施形態では、ワンタイムパスワードの都度変化性のための暗証加工情報の取得を、購買者ではなく販売店が代行しているが、暗証加工情報は、都度変化し購買者と金融機関が共有できる情報であることが最低条件であるので、 これを満たすならば、例えば、金融機関サーバと同期した暗証加工情報を生成する生成機を用いることなどにより、暗証加工情報の送受信を行うことなく、ワンタイムパスワードの生成を行うことができる。

【００３６】さらにまた、上記実施形態では、販売店を経由してワンタイムパスワードを送信しているが、このような形態を取らずに、購買者から金融機関へ直接ワンタイムパスワードを送信することもできる。

【００３７】図１１のフローを用いて示す。購買者が購入開始応答を受信し、ワンタイムパスワードを生成するところまでは、図４に示すフローと同様である。 その後、ユーザID、ワンタイムパスワード、必要に応じて金融機関がトランザクションを特定するための補足情報として暗証加工情報を、 販売店ではなく金融機関へ決済要求として送信する。金融機関は、販売店から決済要求を受信した場合と同様に、ワンタイムパスワードを検証し、検証結果に基づき決済処理を行う。販売店は、決済の可否を金融機関へ問い合わせ、決済結果に基づき取引の成否を判断する。

【００３８】また、購買者から金融機関へ直接ワンタイムパスワードを直接送信する場合には、取引の安全性確保に関して、ワンタイムパスワードの都度変化性は必ずしも必要ではないので、ワンタイムパスワードの生成において、暗証加工情報を用いないことも可能である。

【００３９】尚、上述した実施の形態では、購買者システム、販売店システム、金融機関システムを用いた電子商取引システムを用いて説明したが、購買者と販売店との間でリアルの取引を行った場合等における債権債務の決済にも本発明は適用可能であり、そのような場合は、例えば携帯端末やＩＣカード等により作成されたワンタイムパスワードをユーザが金融機関システムへ直接入力する、または販売店システム等を介することによって、金融機関システムへ決済要求を行えば良い。

【００４０】以上説明したように、本発明によれば、債務者（送金者）が承認している債権者（受領者）との間の決済情報と、債権者が金融機関に通知した債務者との間の決済情報が一致しているか否かを確認することができ、 債務者と債権者が合意した決済情報においてのみ、決済が行われることを確実にすることができる。

【００４１】また、決済機関の口座所有者のみが知ることができる暗証フレーズを知っているもの、つまり、口座所有者本人がワンタイムパスワードを作成したことを確認することができ、口座所有者以外の第三者によるによる取引（いわゆる、 なりすまし）を防止することができる。

【００４２】さらに、暗証加工情報は都度変化するため、正当なワンタイムパスワードは都度変化するので、あるワンタイムパスワードを利用して受領者が決済要求を行えるのを一度だけに限定することができる。

【００４３】この結果、都度変化し、決済情報とリンクした 1 度きり有効なワンタイムパスワードを用いて決済を行うことにより、秘匿性を必要としない情報により、送金者の本人性を確認しながら、安全で確実な決済を実現することが可能となる。また、ワンタイムパスワードの生成には、暗号処理や電子認証書などは必須ではないため、計算機リソースならびに送金者の利用負担軽減を実現することが可能となる。

【００４４】

15

【発明の効果】本発明によれば、決済の確実性、安全性、迅速性のバランスを考慮した決済方法を提供することが可能となる。

【図面の簡単な説明】

【図１】本発明を適用した電子商取引のシステム構成の一例を示すブロック図

【図２】取引DB１７のデータ構成を示す図

【図３】実施形態の取引 DB ３７のデータ構成を示す図

【図４】本発明を適用した電子商取引システムのショッピングフローを示す図

【図５】本発明を適用した電子商取引システムの購買者のフローを示す図

【図６】本発明を適用した電子商取引システムの販売店のフローを示す図

【図７】本発明を適用した電子商取引システムの金融機関のフローを示す図

【図８】実施形態の表示器５５に表示される購入開始要求を送信する際の表示例を示す図

16

＊【図９】実施形態の表示器５５に表示される購入要求を送信する際の表示例を示す図

【図１０】実施形態の表示器５５に表示される購入応答を受信した際の表示例を示す図

【図１１】本発明を適用した電子商取引システムのショッピングフローを示す図（ワンタイムパスワードが販売店を経由しない決済）

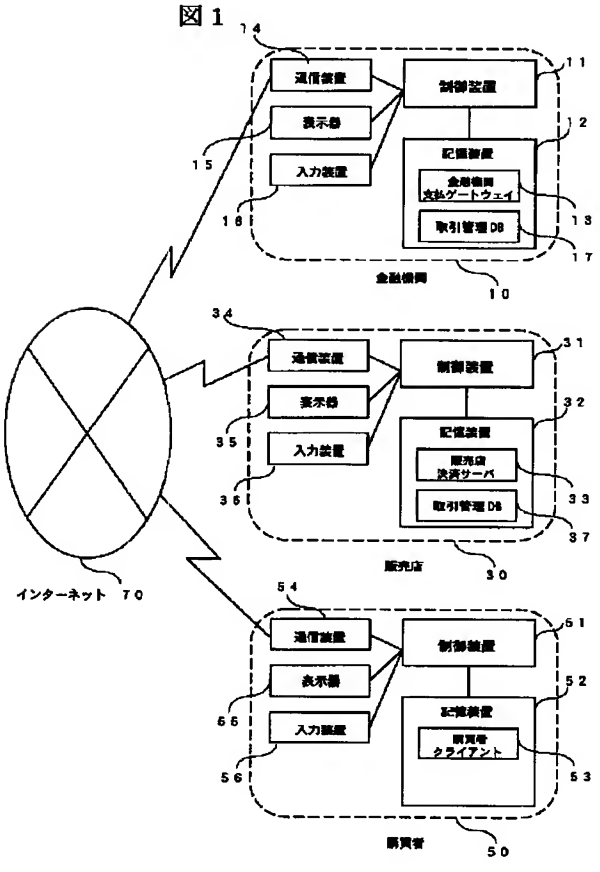
【図１２】ワンタイムパスワードの生成方法を示す図

【符号の説明】

１０…金融機関システム
１３…金融機関支払ゲートウェイ
１７…取引管理ＤＢ
３０…販売店システム
３３…販売店決済サーバ
３７…取引管理ＤＢ
５０…購買者システム
５３…購買者クライアント
７０…インターネット

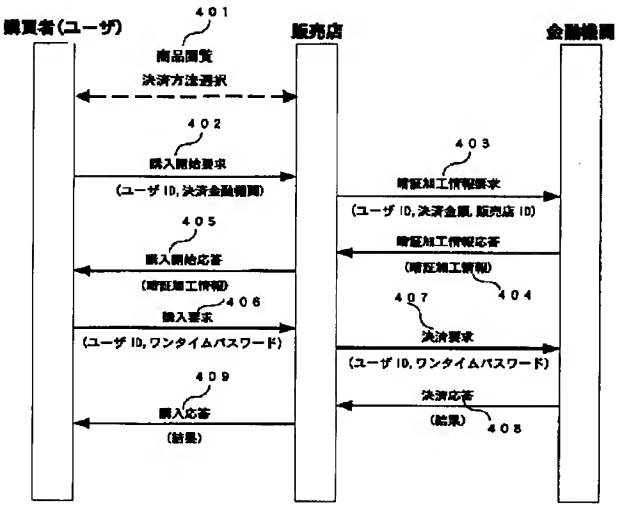
【図１】

図１



【図４】

図４



【図２】

図２

顧客管理データ ２００

２０１ ユーザ識別子	２０２ 顧客口座番号	２０３ 暗証フレーズ
54321A12345	123-2-1234567	Rt4uH52*Vj

販売店管理データ ２１０

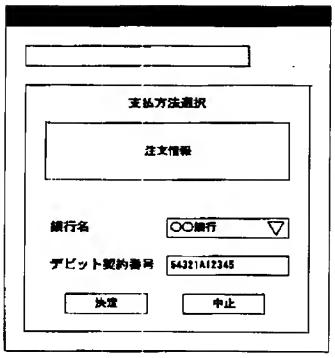
２１１ 販売店識別子	２１２ 販売店口座番号
S234A654	321-1-7654321

取引管理データ ２２０

２２１ 取引識別子	２２２ ユーザ識別子	２２３ 販売店識別子	２２４ 決済金額	２２５ 暗証加工情報
A1999072409876	54321A12345	S234A654	10,000	4H81bd7q

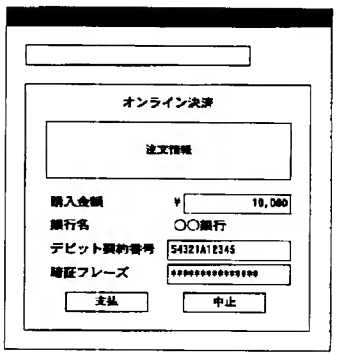
【図８】

図８



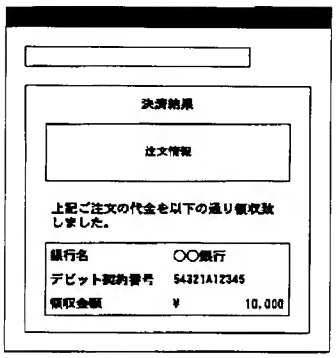
【図９】

図９



【図１０】

図１０



【図３】

図３

決済用
取引管理データ　３００

301 取引識別子	302 決済金融機関	303 ユーザ識別子	304 決済金額	305 取引ステータス
M9876543	○○銀行	54321A12345	10,000	決済要求送信済

金融機関データ　３１０

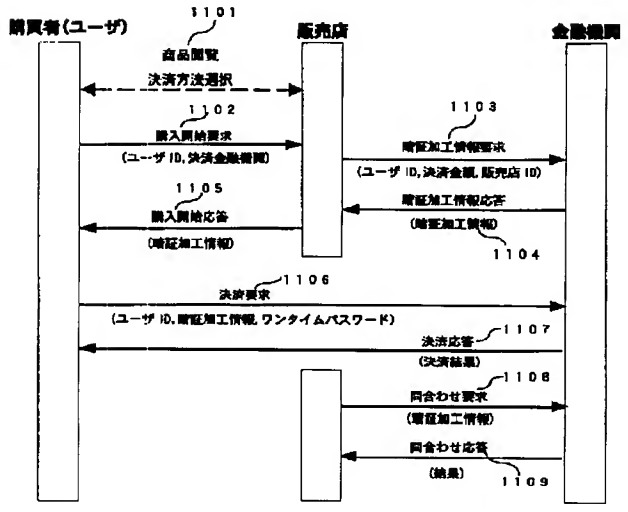
311 決済金融機関	312 接続先情報	313 販売店識別子
○○銀行	www.xxx.yyy	S234A654

商品販売
取引管理データ　３２０

321 取引識別子	322 商品	323 数量	324 送付先
M9876543	G12B	2	東京都...

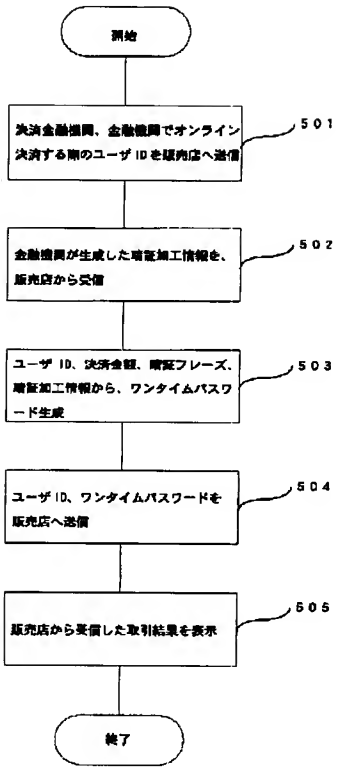
【図１１】

図 11



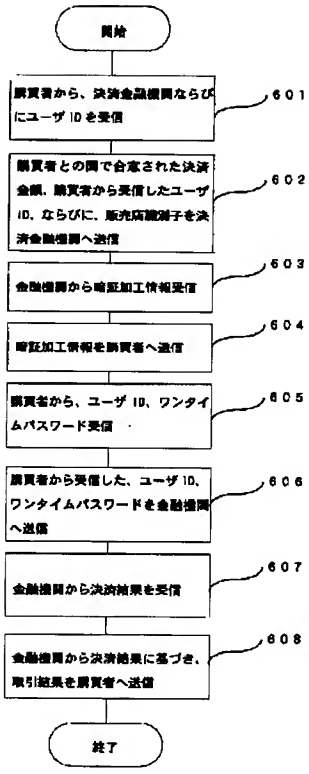
【図５】

図５


開始
決済金融機関、金融機関でオンライン決済する際のユーザ ID を販売店へ送信
501
金融機関が生成した暗証加工情報を、販売店から受信
502
ユーザ ID、決済金額、暗証フレーズ、暗証加工情報から、ワンタイムパスワード生成
503
ユーザ ID、ワンタイムパスワードを販売店へ送信
504
販売店から受信した取引結果を表示
505
終了

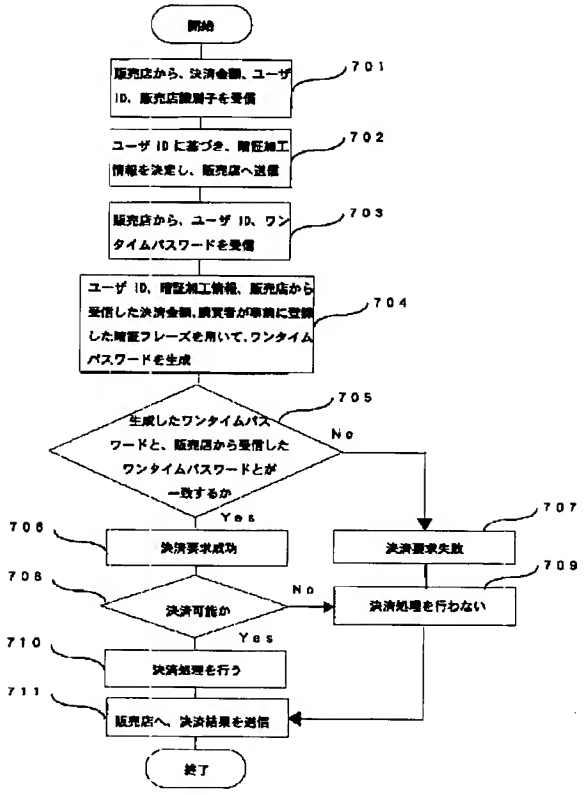
【図６】

図６


開始
購買者から、決済金融機関ならびにユーザ ID を受信
601
購買者との間で合意された決済金額、購買者から受信したユーザ ID、ならびに、販売店識別子を決済金融機関へ送信
602
金融機関から暗証加工情報受信
603
暗証加工情報を購買者へ送信
604
購買者から、ユーザ ID、ワンタイムパスワード受信
605
購買者から受信した、ユーザ ID、ワンタイムパスワードを金融機関へ送信
606
金融機関から決済結果を受信
607
金融機関から決済結果に基づき、取引結果を購買者へ送信
608
終了

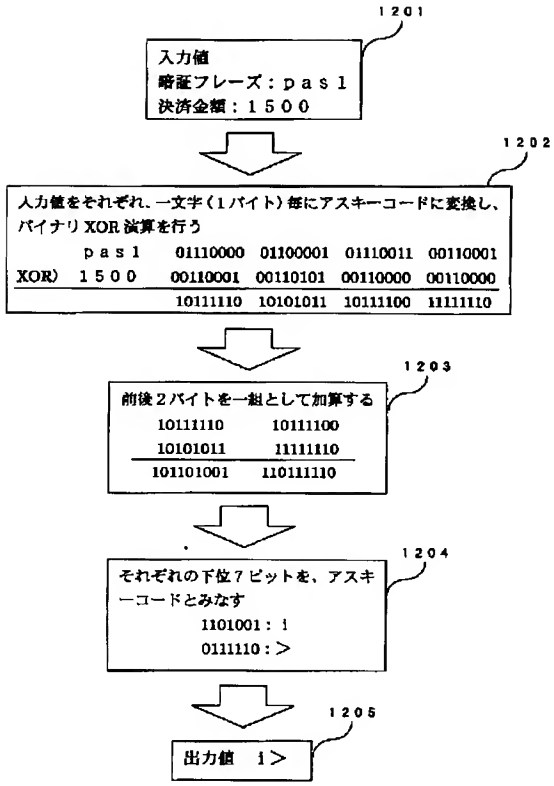
【図７】

図７



【図１２】

図１２



フロントページの続き

(72)発明者　坏　毅
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(72)発明者　武本　敏
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(72)発明者　成島　佳孝
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(72)発明者　川連　嘉晃
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内
(72)発明者　渡邉　清
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション開発本部内

Ｆターム(参考)　5B049 AA05 CC36 CC39 EE23 GG02